Finite Fields and Their Applications 16 (2010) 36–55

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Coset bounds for algebraic geometric codes

Iwan M. Duursma [a,*], Seungkook Park [b,1]

[a] Department of Mathematics, University of Illinois at Urbana-Champaign, United States
[b] Department of Mathematical Sciences, University of Cincinnati, United States

ARTICLE INFO

Article history:
Received 11 March 2009
Revised 24 November 2009
Available online 31 December 2009
Communicated by H. Stichtenoth

Keywords:
Algebraic geometric code
Floor bound
Order bound
Linear secret sharing

ABSTRACT

We develop new coset bounds for algebraic geometric codes. The bounds have a natural interpretation as an adversary threshold for algebraic geometric secret sharing schemes and lead to improved bounds for the minimum distance of an AG code. Our bounds improve both floor bounds and order bounds and provide for the first time a connection between the two types of bounds.

0. Introduction

This paper deals with coset bounds for algebraic geometric codes and their applications to lower bounds for the minimum distance of AG codes as well as for thresholds of algebraic geometric secret sharing schemes. The work was motivated by two important recent results. The first is the complete description of the minimum distance of Hermitian two-point codes by Homma and Kim [1]. The second is the introduction of algebraic geometric linear secret sharing schemes by Chen and Cramer [2].

For algebraic geometric codes, the actual value of the minimum distance is not a priori known and needs to be determined or estimated from the data used in the construction. The best known lower bounds for the minimum distance of an algebraic geometric code are the order bound and the floor bound. In this paper, we obtain improvements for the Beelen version of the order bound [3] and for the Lundell–McCullough version of the floor bound [4]. We note that at the time of revision the Lundell–McCullough floor bound has been extended and improved by Güneri, Stichtenoth and Taşkın [5]. Beelen [3], and independently the second author [6], have shown that the order bound agrees, for Hermitian two-point codes, with the actual minimum distances found by Homma and Kim. To observe numerical improvements of our bounds over previously known bounds we use examples from Suzuki curves.

* Corresponding author.
E-mail addresses: duursma@math.uiuc.edu (I.M. Duursma), napsk71@kias.re.kr (S. Park).
[1] Current address: School of Computational Sciences, Korea Institute for Advanced Study (KIAS), Republic of Korea.

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2009.11.006

An important application of secret sharing schemes is secure multi-party computation, which requires linear secret sharing schemes with a multiplicative property [7,8]. Chen and Cramer proposed to use one-point algebraic geometric codes for secret sharing and they have shown that the obtained algebraic geometric linear secret sharing schemes can be used for efficient secure computation over small fields [2]. Parties can reconstruct a secret uniquely from their shares only if the total number of shares exceeds the adversary threshold of the secret sharing scheme. The algebraic geometric construction of a linear secret sharing scheme guarantees a lower bound for the adversary threshold. The precise value of the threshold is in general not known. We show that the adversary threshold corresponds to the minimum distance between cosets of a code. Our results give improved lower bounds for distances between cosets of an algebraic geometric code, and therefore improved lower bounds for adversary thresholds of algebraic geometric linear secret sharing schemes.

As our main results, we formulate an *ABZ bound for codes* and an *ABZ bound for cosets*. The bounds improve and generalize the Lundell–McCullough floor bound and the Beelen order bound, respectively. The bounds can be used as tools for constructing improved codes as well as improved secret sharing schemes. Our *Main theorem* is an even more general bound. Its main advantage is that it has a short proof and that all other bounds can be obtained as special cases.

The floor bound is independent of the order bound. Algorithms are available for decoding up to half the order bound but not for decoding up to half the floor bound. Beelen [3] gives an example where the floor bound exceeds the order bound. For our generalizations there is a strict hierarchy. The improved order bound, obtained with the ABZ bound for cosets, is at least the ABZ bound for codes, which improves the floor bound. We show that decoding is possible up to half the bound in our main theorem, and therefore up to half of all our bounds. In particular, we obtain for the first time an approach to decode up to half the floor bound.

In Section 1, we describe the use of linear codes for secret sharing and the relation between coset distances and adversary thresholds. Theorem 1.2 gives a general coset bound for linear codes. Appendix A gives a coset decoding procedure that decodes up to half the bound. Algebraic geometric codes are defined in Section 2. Theorem 2.4 gives the ABZ bound for algebraic geometric codes with a first proof based on the AB bound for linear codes. Section 3 gives a geometric characterization of coset distances for algebraic geometric codes. In Section 4 we define, for a divisor C and for a rational point P, a semigroup ideal

$$\Gamma_P(C) = \big\{A\colon\ L(A) \neq L(A-P) \wedge L(A-C) \neq L(A-C-P)\big\}$$

such that the minimal degree for a divisor A in $\Gamma_P(C)$ is a lower bound for the coset distance of an algebraic geometric code. In Section 5, the main theorem gives a lower bound for the degree of a divisor in the semigroup ideal (Theorem 5.3). The bound is formulated in terms of properties of the complement

$$\Delta_P(C) = \big\{A\colon\ L(A) \neq L(A-P) \wedge L(A-C) = L(A-C-P)\big\}.$$

In Section 6, we explain the role of the divisor C for optimizing the order bound (Proposition 6.3). We formulate the ABZ bound for cosets (Theorem 6.5) and we describe its relation to both the order bound (Theorem 6.2) and the floor bound (Theorem 2.3). The material in this paper forms the first half of the preprint [9].

1. Cosets of linear codes

Let $\mathbb{F}$ be a finite field. An $\mathbb{F}$-linear code $\mathcal{C}$ of length n is a linear subspace of $\mathbb{F}^n$. The Hamming distance between two vectors $x, y \in \mathbb{F}^n$ is $d(x, y) = |\{i\colon\ x_i \neq y_i\}|$. The minimum distance of a nontrivial linear code $\mathcal{C}$ is

$$\begin{aligned} d(\mathcal{C}) &= \min\big\{d(x, y)\colon\ x, y \in \mathcal{C},\ x \neq y\big\} \\ &= \min\big\{d(x, 0)\colon\ x \in \mathcal{C},\ x \neq 0\big\}. \end{aligned}$$

If $d(\mathcal{C}) \geqslant 2t+1$ and if $y \in \mathbb{F}^n$ is at distance at most t from $\mathcal{C}$ then there exists a unique word $c \in \mathcal{C}$ with $d(c, y) \leqslant t$.

The Hamming distance between two nonempty subsets $X, Y \subset \mathbb{F}^n$ is the minimum of $\{d(x, y)$: $x \in X,\ y \in Y\}$. For a proper subcode $\mathcal{C}' \subset \mathcal{C}$, the minimum distance of the collection of cosets $\mathcal{C}/\mathcal{C}'$ is

$$\begin{aligned} d(\mathcal{C}/\mathcal{C}') &= \min\{d(x+\mathcal{C}', y+\mathcal{C}')\colon\ x, y \in \mathcal{C},\ x-y \notin \mathcal{C}'\} \\ &= \min\{d(x,0)\colon\ x \in \mathcal{C},\ x \notin \mathcal{C}'\}. \end{aligned}$$

Lemma 1.1. *If $d(\mathcal{C}/\mathcal{C}') \geqslant 2t+1$ and if $y \in \mathbb{F}^n$ is at distance at most t from $\mathcal{C}$ then there exists a unique coset $c+\mathcal{C}' \in \mathcal{C}/\mathcal{C}'$ with $d(c+\mathcal{C}', y+\mathcal{C}') \leqslant t$.*

The dual code $\mathcal{D}$ of $\mathcal{C}$ is the maximal subspace of $\mathbb{F}^n$ that is orthogonal to $\mathcal{C}$ with respect to the standard inner product. To the extension of codes $\mathcal{C}/\mathcal{C}'$ corresponds an extension of dual codes $\mathcal{D}'/\mathcal{D}$ with distance parameter $d(\mathcal{D}'/\mathcal{D})$. For two vectors $x, y \in \mathbb{F}^n$, let $x * y \in \mathbb{F}^n$ denote the Hadamard or coordinate-wise product of the two vectors.

Theorem 1.2 *(Shift bound or coset bound). Let $\mathcal{C}/\mathcal{C}_1$ be an extension of $\mathbb{F}$-linear codes with corresponding extension of dual codes $\mathcal{D}_1/\mathcal{D}$ such that $\dim \mathcal{C}/\mathcal{C}_1 = \dim \mathcal{D}_1/\mathcal{D} = 1$. If there exist vectors $a_1, \ldots, a_w$ and $b_1, \ldots, b_w$ such that*

$$\begin{cases} a_i * b_j \in \mathcal{D} & \text{for } i+j \leqslant w, \\ a_i * b_j \in \mathcal{D}_1 \setminus \mathcal{D} & \text{for } i+j = w+1, \end{cases}$$

then $d(\mathcal{C}/\mathcal{C}_1) \geqslant w$.

Proof. For all $c \in \mathcal{C} \setminus \mathcal{C}_1$ and $a * b \in \mathcal{D}_1 \setminus \mathcal{D}$, c is not orthogonal to $a * b$. To show the nonexistence of a vector $c \in \mathcal{C} \setminus \mathcal{C}_1$ with $d(c, 0) < w$, it suffices to show, for any choice of $w-1$ coordinates, the existence of a vector $a * b \in \mathcal{D}_1 \setminus \mathcal{D}$ that is zero in those coordinates. The conditions show that the vectors $a_1, \ldots, a_w$ are linearly independent, and there exists a nonzero linear combination a of the vectors $a_1, \ldots, a_w$ vanishing at $w-1$ given coordinates (here we use that a system of $w-1$ linear equations in w variables has a nonzero solution). If i is maximal such that a_i has a nonzero coefficient in the linear combination a then $a * b_{w+1-i} \in \mathcal{D}_1 \setminus \mathcal{D}$ is zero in the $w-1$ coordinates. □

Let $y \in \mathbb{F}^n$ be a word at distance at most t from $\mathcal{C}$. For given vectors $a_1, \ldots, a_w$ and $b_1, \ldots, b_w$ such that $w > 2t$, the unique coset $c+\mathcal{C}_1 \in \mathcal{C}/\mathcal{C}_1$ with $d(c+\mathcal{C}_1, y+\mathcal{C}_1) \leqslant t$ can be computed efficiently with the coset decoding procedure in Appendix A. Theorem 1.2 can be used to estimate the minimum distance $d(\mathcal{C}/\mathcal{C}')$ of an extension $\mathcal{C}/\mathcal{C}'$ with $\dim \mathcal{C}/\mathcal{C}' > 1$, after dividing $\mathcal{C}/\mathcal{C}'$ into subextensions.

Lemma 1.3. *Let $\mathcal{C}/\mathcal{C}'$ be an extension of $\mathbb{F}$-linear codes of length n. For $\mathcal{C} \supset \mathcal{C}'' \supset \mathcal{C}'$,*

$$d(\mathcal{C}/\mathcal{C}') = \min\{d(\mathcal{C}/\mathcal{C}''), d(\mathcal{C}''/\mathcal{C}')\}.$$

We will now describe the use of code extensions for secret sharing. Our description focuses on the connection between secret sharing thresholds and coset distances. For the definition and main properties of a general linear secret sharing scheme we refer to [8]. Unless otherwise specified, all code extensions will be of codimension one.

Let $y_1 \in \mathcal{D}_1 \setminus \mathcal{D}$. For a secret $\lambda \in \mathbb{F}$, and for a random vector $y \in \mathcal{D}$, the vector $s = \lambda y_1 + y$ is called a vector of shares for λ. A subset $A \subset \{1, 2, \ldots, n\}$ is said to be qualified for $\mathcal{D}_1 \setminus \mathcal{D}$ if, for any given vector $s = \lambda y_1 + y \in \mathcal{D}_1$, the coefficient λ is uniquely determined by the values of s on the subset of coordinates A. Denote by $\Gamma(\mathcal{D}_1/\mathcal{D})$ the collection of subsets $A \subset \{1, 2, \ldots, n\}$ that are qualified for $\mathcal{D}_1/\mathcal{D}$.

Lemma 1.4. *For $A \subset \{1, 2, \ldots, n\}$, let E_A denote the subspace of $\mathbb{F}^n$ of words that have support in A, and let $\bar{A}$ denote the complement of A in $\{1, 2, \ldots, n\}$. Then*

$$\{A\colon\ \mathcal{C} \cap E_A \neq \mathcal{C}_1 \cap E_A\} \subseteq \Gamma(\mathcal{D}_1/\mathcal{D}) \subseteq \{A\colon\ \mathcal{D}_1 \cap E_{\bar{A}} = \mathcal{D} \cap E_{\bar{A}}\}.$$

Proof. For the first inclusion, assume that $\mathcal{C} \cap E_A \neq \mathcal{C}_1 \cap E_A$ and let $r \in \mathcal{C} \setminus \mathcal{C}_1$ be a codeword with support in A. Then, for any given vector $s = \lambda y_1 + y \in \mathcal{D}_1$, we can compute $r \cdot s$ using only the values of s on A. Moreover, $r \cdot s = r \cdot (\lambda y_1 + y) = \lambda(r \cdot y_1)$. And since $(r \cdot y_1) \neq 0$, we obtain $\lambda = (r \cdot s)/(r \cdot y_1)$. For the other inclusion, assume that $\mathcal{D}_1 \cap E_{\bar{A}} \neq \mathcal{D} \cap E_{\bar{A}}$ and let $s' = y_1 + y \in \mathcal{D}_1 \setminus \mathcal{D}$ be a codeword that is zero on A. Then the values on A are the same for the vector $s = \lambda y_1 + y \in \mathcal{D}_1$ and for its translates $s + \mu s'$. Thus λ cannot be determined from the values of s on A and $A \notin \Gamma(\mathcal{D}_1/\mathcal{D})$. □

The inclusions in the lemma hold with equality. To see this we use the following duality.

Lemma 1.5. *Let $A \subset \{1, 2, \ldots, n\}$. There exists a word $r \in \mathcal{C} \setminus \mathcal{C}_1$ with support in A if and only if there exists no word $s \in \mathcal{D}_1 \setminus \mathcal{D}$ with support in $\bar{A}$.*

Proof. The exact sequences

$$0 \longrightarrow \mathcal{C} \cap E_A/\mathcal{C}_1 \cap E_A \longrightarrow \mathcal{C}/\mathcal{C}_1 \longrightarrow \mathcal{C} + E_A/\mathcal{C}_1 + E_A \longrightarrow 0,$$
$$0 \longrightarrow \mathcal{D}_1 \cap E_{\bar{A}}/\mathcal{D} \cap E_{\bar{A}} \longrightarrow \mathcal{D}_1/\mathcal{D} \longrightarrow \mathcal{D}_1 + E_{\bar{A}}/\mathcal{D} + E_{\bar{A}} \longrightarrow 0,$$

are in duality via $V \mapsto V^* = \mathrm{Hom}(V, \mathbb{F})$. And

$$(\dim \mathcal{C} \cap E_A/\mathcal{C}_1 \cap E_A) + (\dim \mathcal{D}_1 \cap E_{\bar{A}}/\mathcal{D} \cap E_{\bar{A}}) = \dim \mathcal{C}/\mathcal{C}_1 = 1. \qquad \square$$

Denote by $\Delta(\mathcal{D}_1/\mathcal{D})$ the collection of unqualified subsets for $\mathcal{D}_1/\mathcal{D}$. Together the lemmas give the following characterization of qualified and unqualified subsets.

Theorem 1.6. *Let $\mathcal{C}/\mathcal{C}_1$ and $\mathcal{D}_1/\mathcal{D}$ be dual extensions of $\mathbb{F}$-linear codes of length n. For $A \subset \{1, 2, \ldots, n\}$, let E_A be the subset of $\mathbb{F}^n$ of all vectors with support in A and let $\bar{A} = \{1, 2, \ldots, n\} \setminus A$. Then*

$$\{A\colon\ \mathcal{C} \cap E_A \neq \mathcal{C}_1 \cap E_A\} = \Gamma(\mathcal{D}_1/\mathcal{D}) = \{A\colon\ \mathcal{D}_1 \cap E_{\bar{A}} = \mathcal{D} \cap E_{\bar{A}}\},$$
$$\{A\colon\ \mathcal{D}_1 \cap E_{\bar{A}} \neq \mathcal{D} \cap E_{\bar{A}}\} = \Delta(\mathcal{D}_1/\mathcal{D}) = \{A\colon\ \mathcal{C} \cap E_A = \mathcal{C}_1 \cap E_A\}.$$

Moreover,

$$A \in \Gamma(\mathcal{C}/\mathcal{C}_1) \quad \Leftrightarrow \quad \bar{A} \in \Delta(\mathcal{D}_1/\mathcal{D}) \quad \text{and} \quad A \in \Delta(\mathcal{C}/\mathcal{C}_1) \quad \Leftrightarrow \quad \bar{A} \in \Gamma(\mathcal{D}_1/\mathcal{D}).$$

Proof. With Lemma 1.5, the inclusions in Lemma 1.4 become equalities. The other claims follow immediately. □

Corollary 1.7. *The smallest qualified subset for $\mathcal{D}_1/\mathcal{D}$ is of size*

$$\min\{|A|\colon\ A \in \Gamma(\mathcal{D}_1/\mathcal{D})\} = d(\mathcal{C}/\mathcal{C}_1).$$

The largest unqualified subset for $\mathcal{D}_1/\mathcal{D}$ is of size

$$\max\{|A|\colon\ A \in \Delta(\mathcal{D}_1/\mathcal{D})\} = n - d(\mathcal{D}_1/\mathcal{D}).$$

2. Algebraic geometric codes

Let $X/\mathbb{F}$ be an algebraic curve (absolutely irreducible, smooth, projective) of genus g over a finite field $\mathbb{F}$. Let $\mathbb{F}(X)$ be the function field of $X/\mathbb{F}$ and let $\Omega(X)$ be the module of rational differentials of $X/\mathbb{F}$. Given a divisor E on X defined over $\mathbb{F}$, let $L(E)$ denote the vector space over $\mathbb{F}$ of functions $f \in \mathbb{F}(X) \setminus \{0\}$ with $(f) + E \geqslant 0$ together with the zero function. The dimension of $L(E)$ is denoted by $l(E)$. Let $\Omega(E)$ denote the vector space over $\mathbb{F}$ of differentials $\omega \in \Omega(X) \setminus \{0\}$ with $(\omega) \geqslant E$ together with the zero differential. Let K represent the canonical divisor class.

For n distinct rational points $P_1, \ldots, P_n$ on X and for disjoint divisors $D = P_1 + \cdots + P_n$ and G, the geometric Goppa codes $C_L(D, G)$ and $C_\Omega(D, G)$ are defined as the images of the maps

$$\alpha_L : L(G) \longrightarrow \mathbb{F}^n, \qquad f \mapsto \big(f(P_1), \ldots, f(P_n)\big),$$
$$\alpha_\Omega : \Omega(G - D) \longrightarrow \mathbb{F}^n, \qquad \omega \mapsto \big(\operatorname{res}_{P_1}(\omega), \ldots, \operatorname{res}_{P_n}(\omega)\big).$$

The maps establish isomorphisms $L(G)/L(G - D) \simeq C_L(D, G)$ and $\Omega(G - D)/\Omega(G) \simeq C_\Omega(D, G)$. With the Residue theorem, the images are orthogonal subspaces of $\mathbb{F}^n$. With the Riemann–Roch theorem they are maximal orthogonal subspaces.

There exists a nonzero word in $C_L(D, G)$ with support in A, for $0 \leqslant A \leqslant D$, if and only if $L(G - D + A)/L(G - D) \neq 0$. There exists a nonzero word in $C_\Omega(D, G)$ with support in A, for $0 \leqslant A \leqslant D$, if and only if $\Omega(G - A)/\Omega(G) \neq 0$ if and only if $L(K - G + A)/L(K - G) \neq 0$.

Proposition 2.1.

$$d\big(C_L(D, G)\big) = \min\big\{\deg A\colon\ 0 \leqslant A \leqslant D \bigm| L(A - C) \neq L(-C)\big\}, \quad \text{for } C = D - G,$$
$$d\big(C_\Omega(D, G)\big) = \min\big\{\deg A\colon\ 0 \leqslant A \leqslant D \bigm| L(A - C) \neq L(-C)\big\}, \quad \text{for } C = G - K.$$

Theorem 2.2 *(Goppa bound). A nonzero word in $C_L(D, G)$ has weight $w \geqslant \deg(D - G)$. A nonzero word in $C_\Omega(D, G)$ has weight $w \geqslant \deg(G - K)$.*

The following bound improves on the Goppa bound in special cases.

Theorem 2.3 *(Floor bound). (See [4].) Let $G = K + C = A + B + Z$, for $Z \geqslant 0$ such that $L(A + Z) = L(A)$ and $L(B + Z) = L(B)$. For D with $D \cap Z = \emptyset$, a nonzero word in $C_\Omega(D, G)$ has weight at least $\deg C + \deg Z$.*

Most algebraic bounds for the minimum distance of a linear code rely on one of two basic arguments. In the paper [10] on cyclic codes they were named the AB bound and the Shift bound. We obtain the following bound, which includes the floor bound, using the AB bound argument in combination with the Goppa bound.

Theorem 2.4 *(ABZ bound for codes). Let $G = K + C = A + B + Z$, for $Z \geqslant 0$. For D with $D \cap Z = \emptyset$, a nonzero word in $C_\Omega(D, G)$ has weight $w \geqslant l(A) - l(A - C) + l(B) - l(B - C)$.*

Proof. We may assume that A and B are disjoint from D. Since $Z \geqslant 0$ and $D \cap Z = \emptyset$, the code $C_L(D, G)$ contains the code $C_L(D, A + B)$ as a subcode. Thus $C_L(D, A) * C_L(D, B) \perp C_\Omega(D, G)$. Let $c \in C_\Omega(D, G)$ have support $D' \leqslant D$. Since $c * C_L(D, A) \simeq C_L(D', A)$ and $c * C_L(D, B) \simeq C_L(D', B)$,

$$\begin{aligned}\deg D' &= \dim\big(c * \mathbb{F}^n\big) \geqslant \dim\big(c * C_L(D, A)\big) + \dim\big(c * C_L(D, B)\big)\\ &= \dim\big(C_L\big(D', A\big)\big) + \dim\big(C_L\big(D', B\big)\big)\\ &= l(A) - l\big(A - D'\big) + l(B) - l\big(B - D'\big).\end{aligned}$$

Since $c \in C_\Omega(D, G)$ has support D', there exists a nonzero differential $\eta \in \Omega(G - D') \simeq L(D' - C)$, that is, $L(D' - C) \neq 0$. Thus there exists an effective divisor $E \geqslant 0$ such that $D' - C \sim E$. Hence $l(A - C) = l(A - D' + E) \geqslant l(A - D')$ and $l(B - C) = l(B - D' + E) \geqslant l(B - D')$. Therefore

$$\begin{aligned}\deg D' &\geqslant l(A) - l\big(A - D'\big) + l(B) - l\big(B - D'\big)\\ &\geqslant l(A) - l(A - C) + l(B) - l(B - C). \qquad \square\end{aligned}$$

It is easy to see, using the Riemann–Roch theorem, that the choice $Z = 0$ returns the Goppa bound. Improvements of the Goppa bound are obtained only if the divisors A, B, and Z, are carefully chosen. For the special case $L(A + Z) = L(A)$ and $L(B + Z) = L(B)$, we recover the floor bound. In that case, for $K + C = A + B + Z$,

$$\begin{aligned}&l(A) - l(A - C) + l(B) - l(B - C)\\ &\quad = l(A + Z) - l(K - B - Z) + l(B + Z) - l(K - A - Z)\\ &\quad = \deg(A + Z) + \deg(B + Z) + 2 - 2g = \deg C + \deg Z.\end{aligned}$$

Example 2.5. The Suzuki curve over the field of 32 elements is defined by the equation $y^{32} + y = x^4(x^{32} + x)$. The curve has $32^2 + 1$ rational points and genus 124. For any two rational points P and Q, the divisors $41P$ and $41Q$ are equivalent and we denote their class by H. The canonical divisor class $K = 6H$. For the code $C_\Omega(D, K + 9P + 9Q)$, the Goppa bound gives $d \geqslant 18$. An optimal choice for the floor bound is $Z = 3P + 3Q$, $A = 2H + 6P + 6Q$ and $B = 4H$, which gives $d \geqslant 24$. An optimal choice for the ABZ bound is $Z = 9P + 9Q$, $A = 2H$ and $B = 4H$. With $\dim L(2H)/L(2H - C) = 10$ and $\dim L(4H)/L(4H - C) = 18$ it gives $d \geqslant 28$.

3. Cosets of algebraic geometric codes

Let $\mathcal{D} = C_\Omega(D, G)$ and $\mathcal{C} = C_L(D, G)$ be dual algebraic geometric codes. For a rational point P disjoint from $D = P_1 + \cdots + P_n$, let

$$\begin{aligned}\mathcal{D}_1/\mathcal{D} &= C_\Omega(D, G - P)/C_\Omega(D, G),\\ \mathcal{C}/\mathcal{C}_1 &= C_L(D, G)/C_L(D, G - P),\end{aligned}$$

be dual extensions of codes. When $\dim \mathcal{C}/\mathcal{C}_1 = \dim \mathcal{D}_1/\mathcal{D} = 1$, the extensions can be used for secret sharing as described in Section 1. Let $\omega \in \Omega(G - D - P) \setminus \Omega(G - D)$. For a secret $s \in \mathbb{F}$ and for a random $\eta \in \Omega(G - D)$ the share of player i is $s_i = s \operatorname{res}_{P_i}(\omega) + \operatorname{res}_{P_i}(\eta)$. A divisor $0 \leqslant A \leqslant D$ is called qualified for $\mathcal{D}_1/\mathcal{D}$ if the shares $\{s_i\colon\ P_i \in \operatorname{supp}(A)\}$ determine s uniquely. Let $f \in L(G) \setminus L(G - P)$. For a secret $s \in \mathbb{F}$ and for a random $h \in L(G - P)$ the share of player i is $s_i = sf(P_i) + h(P_i)$. A divisor $0 \leqslant A \leqslant D$ is called qualified for $\mathcal{C}/\mathcal{C}_1$ if the shares $\{s_i\colon\ P_i \in \operatorname{supp}(A)\}$ determine s uniquely. The quotients $\mathcal{D}_1/\mathcal{D}$ and $\mathcal{C}/\mathcal{C}_1$ are special case of extensions of linear codes and Theorem 1.6 can be used to determine their qualified and unqualified subsets. Proposition 3.1 and Proposition 3.2 give equivalent descriptions in terms of divisors. For a divisor $0 \leqslant A \leqslant D$, let E_A be the subset of $\mathbb{F}^n$ of all vectors that are zero outside A.

Proposition 3.1. *For the extension of codes $\mathcal{D}_1/\mathcal{D} = C_\Omega(D, G - P)/C_\Omega(D, G)$, where $D = P_1 + \cdots + P_n$ is a sum of n distinct rational points, G is a divisor disjoint from D, and P is a rational point disjoint from D,*

$$\begin{aligned}\Gamma(\mathcal{D}_1/\mathcal{D}) &= \{0 \leqslant A \leqslant D\colon\ \mathcal{C} \cap E_A \neq \mathcal{C}_1 \cap E_A\}\\ &= \big\{0 \leqslant A \leqslant D\colon\ L(G - D + A) \neq L(G - D + A - P)\big\},\end{aligned}$$

$$\begin{aligned}\Delta(\mathcal{D}_1/\mathcal{D}) &= \{0 \leqslant A \leqslant D\colon\ \mathcal{C} \cap E_A = \mathcal{C}_1 \cap E_A\} \\ &= \big\{0 \leqslant A \leqslant D\colon\ L(G - D + A) = L(G - D + A - P)\big\}.\end{aligned}$$

Proposition 3.2. *For the extension of codes $\mathcal{C}/\mathcal{C}_1 = C_L(D, G)/C_L(D, G - P)$, where $D = P_1 + \cdots + P_n$ is a sum of n distinct rational points, G is a divisor disjoint from D, and P is a rational point disjoint from D,*

$$\begin{aligned}\Gamma(\mathcal{C}/\mathcal{C}_1) &= \{0 \leqslant A \leqslant D\colon\ \mathcal{D}_1 \cap E_A \neq \mathcal{D} \cap E_A\} \\ &= \big\{0 \leqslant A \leqslant D\colon\ \Omega(G - A - P) \neq \Omega(G - A)\big\}, \\ \Delta(\mathcal{C}/\mathcal{C}_1) &= \{0 \leqslant A \leqslant D\colon\ \mathcal{D}_1 \cap E_A = \mathcal{D} \cap E_A\} \\ &= \big\{0 \leqslant A \leqslant D\colon\ \Omega(G - A - P) = \Omega(G - A)\big\}.\end{aligned}$$

The propositions are related via the dualities $A \in \Gamma(\mathcal{D}_1/\mathcal{D})$ if and only if $D - A \in \Delta(\mathcal{C}/\mathcal{C}_1)$ and $A \in \Gamma(\mathcal{C}/\mathcal{C}_1)$ if and only if $D - A \in \Delta(\mathcal{D}_1/\mathcal{D})$ (as in Theorem 1.6). The minimal degree of a divisor $A \in \Gamma(\mathcal{D}_1/\mathcal{D})$ or $A \in \Gamma(\mathcal{C}/\mathcal{C}_1)$ is given by the coset distance $d(\mathcal{C}/\mathcal{C}_1)$ or $d(\mathcal{D}_1/\mathcal{D})$, respectively (as in Corollary 1.7).

Proposition 3.3.

$$\begin{aligned}d(\mathcal{C}/\mathcal{C}_1) &= \min\big\{\deg A\colon\ 0 \leqslant A \leqslant D \,\big|\, L(A - C) \neq L(A - C - P)\big\}, \quad \text{for } C = D - G, \\ d(\mathcal{D}_1/\mathcal{D}) &= \min\big\{\deg A\colon\ 0 \leqslant A \leqslant D \,\big|\, L(A - C) \neq L(A - C - P)\big\}, \quad \text{for } C = G - K - P.\end{aligned}$$

This motivates the following definition. For a given divisor C and a point P, let

$$\Gamma_P(C) = \big\{A\colon\ L(A) \neq L(A - P) \wedge L(A - C) \neq L(A - C - P)\big\},$$

and let $\gamma_P(C)$ be the minimal degree for a divisor $A \in \Gamma_P(C)$. So that $\gamma_P(C) \geqslant \max\{0, \deg C\}$.

Theorem 3.4. *For the extensions of codes $\mathcal{D}_1/\mathcal{D} = C_\Omega(D, G - P)/C_\Omega(D, G)$ and $\mathcal{C}/\mathcal{C}_1 = C_L(D, G)/C_L(D, G - P)$,*

$$\begin{aligned}A \in \Gamma(\mathcal{D}_1/\mathcal{D}) &\Rightarrow \deg A \geqslant \gamma_P(D - G) \geqslant n - \deg G, \\ A \in \Delta(\mathcal{D}_1/\mathcal{D}) &\Rightarrow \deg A \leqslant n - \gamma_P(G - K - P) \leqslant n - \deg G + 2g - 1, \\ A \in \Gamma(\mathcal{C}/\mathcal{C}_1) &\Rightarrow \deg A \geqslant \gamma_P(G - K - P) \geqslant \deg G - 2g + 1, \\ A \in \Delta(\mathcal{C}/\mathcal{C}_1) &\Rightarrow \deg A \leqslant n - \gamma_P(D - G) \leqslant \deg G.\end{aligned}$$

The lower bounds for $\deg A$ that are obtained with $\gamma_P(D - G)$ and $\gamma_P(G - K - P)$ use the assumption $L(A) \neq L(A - P)$ instead of the stronger assumption $0 \leqslant A \leqslant D$. Thus, when the bound for $\deg A$ is not attained by divisors A of the form $0 \leqslant A \leqslant D$, the bounds will not be optimal. Essentially, we separate the problem of finding a small $A \in \Gamma(\mathcal{D}_1/\mathcal{D})$ into two parts: a geometric part that considers all effective divisors A not containing P, and an arithmetic part that verifies if A can be represented by a divisor with $0 \leqslant A \leqslant D$. Only the first part is considered in this paper.

We include an alternative geometric description of the qualified sets for $\mathcal{D}_1/\mathcal{D}$ and $\mathcal{C}/\mathcal{C}_1$. Let P have multiplicity e in G, and let t be a fixed local parameter for P. For $\dim \mathcal{D}_1/\mathcal{D} = \dim \mathcal{C}/\mathcal{C}_1 = 1$, we have isomorphisms

$$\Omega(G-D-P)/\Omega(G-D) \xrightarrow{\sim} \mathbb{F}, \qquad \omega \mapsto \operatorname{res}_P\big(t^{-e}\omega\big),$$
$$L(G)/L(G-P) \xrightarrow{\sim} \mathbb{F}, \qquad f \mapsto \big(t^e f\big)(P).$$

Lemma 3.5. *For $\omega \in \Omega(G-D-P)$, the residue $\operatorname{res}_P(t^{-e}\omega)$ is uniquely determined by the values $\{\operatorname{res}_P(\omega)(P_i)\colon\ P_i \in A\}$, for $0 \leqslant A \leqslant D$, if and only if $\Omega(G-D+A-P) = \Omega(G-D+A)$.*

With $\Omega(G-D+A-P) = \Omega(G-D+A)$ if and only if $L(G-D+A) \neq L(G-D+A-P)$ the subsets A in the lemma agree with $\Gamma(\mathcal{D}_1/\mathcal{D})$ in Proposition 3.1.

Lemma 3.6. *For $f \in L(G)$, the value $(t^e f)(P)$ is uniquely determined by the values $\{f(P_i)\colon\ P_i \in A\}$, for $0 \leqslant A \leqslant D$, if and only if $L(G-A) = L(G-A-P)$.*

With $L(G-A) = L(G-A-P)$ if and only if $\Omega(G-A-P) \neq \Omega(G-A)$ the subsets A in the lemma agree with $\Gamma(\mathcal{C}/\mathcal{C}_1)$ in Proposition 3.2.

4. Semigroup ideals

Let $X/\mathbb{F}$ be a curve over a field $\mathbb{F}$ and let $\operatorname{Pic}(X)$ be the group of divisor classes. Let $\Gamma = \{A\colon\ L(A) \neq 0\}$ be the semigroup of effective divisor classes. For a given rational point $P \in X$, let $\Gamma_P = \{A\colon\ L(A) \neq L(A-P)\}$ be the semigroup of effective divisor classes with no base point at P. Call $A \in \Gamma_P$ a P-denominator for the divisor class $C \in \operatorname{Pic}(X)$ if $A - C \in \Gamma_P$. So that $A-(A-C)$ expresses C as the difference of two effective divisor classes without base point at P. The P-denominators for C form the Γ_P-ideal

$$\Gamma_P(C) = \{A \in \Gamma_P\colon\ A - C \in \Gamma_P\}.$$

The ideal structure of the semigroup $\Gamma_P(C)$ amounts to the property $A + E \in \Gamma_P(C)$ whenever $A \in \Gamma_P(C)$ and $E \in \Gamma_P$. The Γ_P-ideal of P-numerators for C is the ideal

$$\Gamma_P(-C) = \{A \in \Gamma_P\colon\ A + C \in \Gamma_P\}.$$

Clearly, A is a P-denominator for C if and only if $A-C$ is a P-numerator for C, that is

$$A \in \Gamma_P(C) \quad \Leftrightarrow \quad A - C \in \Gamma_P(-C).$$

The minimal degree $\gamma_P(C)$ of a P-denominator for C is defined as

$$\gamma_P(C) = \min\big\{\deg A\colon\ A \in \Gamma_P(C)\big\}.$$

The minimal degrees satisfy

$$\gamma_P(C) - \gamma_P(-C) = \deg C.$$

The denominator and numerator terminology is borrowed from the ideal interpretation of divisors. Let O be the ring of rational functions in $\mathbb{F}(X)$ that are regular outside P. For effective divisors A and B disjoint from P, the fractional O-ideal $\bigcup_{i\geqslant 0} L(iP-(B-A)) = JI^{-1}$ is the quotient of the integral O-ideals $J = \bigcup_{i\geqslant 0} L(iP-B)$ and $I = \bigcup_{i\geqslant 0} L(iP-A)$. To a denominator A of smallest degree corresponds an ideal I of smallest norm.

If either $C \in \Gamma_P$ or $-C \in \Gamma_P$ then the conditions $A \in \Gamma_P$ and $A - C \in \Gamma_P$ are dependent.

Proposition 4.1. *For a divisor C on a curve X of genus g, $\gamma_P(C) \geqslant \max\{0, \deg C\}$. Moreover,*

$$\gamma_P(C) = 0 \quad \Leftrightarrow \quad -C \in \Gamma_P \quad \Leftrightarrow \quad \Gamma_P(C) = \Gamma_P,$$
$$\gamma_P(C) = \deg C \quad \Leftrightarrow \quad C \in \Gamma_P \quad \Leftrightarrow \quad \Gamma_P(-C) = \Gamma_P.$$

The inequality is strict if and only if $C, -C \notin \Gamma_P$ only if $|\deg C| < 2g$.

For suitable choices of the divisor C, the parameter $\gamma_P(C)$ gives a lower bound for the coset distance of an algebraic geometric code (Proposition 3.3) and therefore bounds for the access structure of an algebraic geometric linear secret sharing scheme (Theorem 3.4). Proposition 4.1 shows that we can expect improvements over the trivial lower bound $\gamma_P(C) \geqslant \deg C$ that is used for Theorem 3.4 only if P is a base point for the divisor C.

Let S be a finite set of rational points that includes P. For $\Gamma_S = \bigcap_{Q \in S} \Gamma_Q$, let $\Gamma_P(C; S) = \Gamma_P(C) \cap \Gamma_S = \{A \in \Gamma_S\colon\ A - C \in \Gamma_P\}$, and let $\gamma_P(C; S)$ be the minimal degree for a divisor $A \in \Gamma_P(C; S)$.

Lemma 4.2. *For a given set of rational points S that includes P, and for extensions of algebraic geometric codes $C_\Omega(D, G - P)/C_\Omega(D, G)$ and $C_L(D, G)/C_L(D, G - P)$ defined with a divisor $D = P_1 + \cdots + P_n$ disjoint from S,*

$$d\big(C_L(D, G)/C_L(D, G - P)\big) \geqslant \gamma_P(C; S), \quad \text{for } C = D - G,$$
$$d\big(C_\Omega(D, G - P)/C_\Omega(D, G)\big) \geqslant \gamma_P(C; S), \quad \text{for } C = G - K - P.$$

Proof. Proposition 3.3. □

To obtain similar estimates for the minimum distance of an algebraic geometric code, we use Proposition 2.1. Define the Γ_S-ideals $\Gamma^*(C; S) \subseteq \Gamma(C; S)$,

$$\Gamma^*(C; S) = \big\{A \in \Gamma_S\colon\ L(A - C) \neq L(-C)\big\},$$
$$\Gamma(C; S) = \big\{A \in \Gamma_S\colon\ L(A - C) \neq 0\big\}.$$

Let $\gamma^*(C; S)$ (resp. $\gamma(C; S)$) denote the minimal degree for a divisor $A \in \Gamma^*(C; S)$ (resp. $A \in \Gamma(C, S)$).

Lemma 4.3. *For a given set of rational points S, and for algebraic geometric codes $C_L(D, G)$ and $C_\Omega(D, G)$ defined with a divisor $D = P_1 + \cdots + P_n$ disjoint from S,*

$$d\big(C_L(D, G)\big) \geqslant \gamma^*(C; S) \geqslant \gamma(C; S), \quad \text{for } C = D - G,$$
$$d\big(C_\Omega(D, G)\big) \geqslant \gamma^*(C; S) \geqslant \gamma(C; S), \quad \text{for } C = G - K.$$

For $L(-C) = 0$, $\gamma^*(C; S) = \gamma(C; S)$.

Proof. Proposition 2.1. □

The condition $L(-C) = 0$ holds in all cases where the Goppa lower bound $d \geqslant \deg C$ (Theorem 2.2) is positive. We give lower bounds for $\gamma(C; S)$ using lower bounds for $\gamma_P(C; S)$. With a minor modification, we obtain lower bounds for $\gamma^*(C; S)$.

Lemma 4.4. *Let S be a finite set of rational points. For a divisor C, and for a rational point $P \in S$,*

$$\Gamma(C;S) = \Gamma_P(C;S) \cup \Gamma(C+P;S),$$
$$\Gamma^*(C;S) \subseteq \Gamma_P(C;S) \cup \Gamma^*(C+P;S).$$

Moreover, for $-C \in \Gamma_P$,

$$\Gamma^*(C;S) \subseteq \Gamma^*(C+P;S).$$

Proof. For the equality, $L(A-C) \neq 0$ if and only if $L(A-C) \neq L(A-C-P)$ or $L(A-C-P) \neq 0$. For the inclusion, $L(A-C) \neq L(-C)$ only if $L(A-C) \neq L(A-C-P)$ or $L(A-C-P) \neq L(-C-P)$. Finally, for $A \in \Gamma^*(C;S)$ such that $-C \in \Gamma_P$, we have $\dim L(A-C)/L(-C-P) > 1$, and thus $L(A-C-P) \neq L(-C-P)$. So that $A \in \Gamma^*(C+P;S)$. □

Proposition 4.5. *Let S be a finite set of rational points. For a divisor C, and for a rational point $P \in S$,*

$$\gamma(C;S) \geqslant \min\{\gamma_P(C;S), \gamma(C+P;S)\},$$
$$\gamma^*(C;S) \geqslant \min\{\gamma_P(C;S), \gamma^*(C+P;S)\} \setminus \{0\}.$$

Proof. In general $\gamma^*(C;S) > 0$. And $\gamma_P(C;S) = 0$ only if $\gamma_P(C) = 0$ if and only if $-C \in \Gamma_P$, in which case we can omit $\gamma_P(C;S)$ before taking the minimum. □

5. Main theorem

For a given curve $X/\mathbb{F}$, let $C \in \mathrm{Pic}(X)$ be a divisor class and let P be a rational point on X. For the semigroup $\Gamma_P = \{A\colon\ L(A) \neq L(A-P)\}$ and the Γ_P-ideal

$$\Gamma_P(C) = \{A \in \Gamma_P\colon\ A - C \in \Gamma_P\},$$

define the complement

$$\Delta_P(C) = \{A \in \Gamma_P\colon\ A - C \notin \Gamma_P\}.$$

Lemma 5.1.

$$\Delta_P(C) = \emptyset \quad \Leftrightarrow \quad \Gamma_P(C) = \Gamma_P \quad \Leftrightarrow \quad -C \in \Gamma_P.$$

Let X be of genus g and let K represent the canonical divisor class.

Lemma 5.2. *In general,*

$$A \in \Delta_P(C) \quad \Leftrightarrow \quad K + C + P - A \in \Delta_P(C).$$

For $A \in \Delta_P(C)$,

$$\min\{0, \deg C\} \leqslant \deg A \leqslant \max\{2g-1, \deg C + 2g - 1\}.$$

Proof. This follows from the definition together with the Riemann–Roch theorem. □

The following is the analogue of Theorem 1.2 in the language of divisors.

Theorem 5.3 *(Coset bound for divisors). Let* $\{A_1 \leqslant A_2 \leqslant \cdots \leqslant A_w\} \subset \Delta_P(C)$ *be a sequence of divisors with* $A_{i+1} \geqslant A_i + P$*, for* $i = 1, \ldots, w-1$*. Then* $\deg A \geqslant w$*, for every divisor* $A \in \Gamma_P(C)$ *with support disjoint from* $A_w - A_1$*, that is*

$$\gamma_P(C; A_w - A_1) \geqslant w.$$

Proof. Let $A \in \Gamma_P$. After replacing the sequence with an equivalent sequence if necessary, we may assume that $A_1, A_2, \ldots, A_w$ are disjoint from A. We obtain two sequences of subspaces.

$$\begin{aligned} L(A_w) &\supsetneq L(A_w - P) \supseteq L(A_{w-1}) \supsetneq L(A_{w-1} - P) \supseteq \cdots \supseteq L(A_2) \\ &\supsetneq L(A_2 - P) \supseteq L(A_1) \supsetneq L(A_1 - P), \\ \Omega(A_w - C) &\subsetneq \Omega(A_w - C - P) \subseteq \Omega(A_{w-1} - C) \subsetneq \Omega(A_{w-1} - C - P) \subseteq \cdots \subset \Omega(A_2 - C) \\ &\subsetneq \Omega(A_2 - C - P) \subseteq \Omega(A_1 - C) \subsetneq \Omega(A_1 - C - P). \end{aligned}$$

For $i = 1, 2, \ldots, w$, choose

$$f_i \in L(A_i) \setminus L(A_i - P) \quad \text{and} \quad \eta_i \in \Omega(A_i - C - P) \setminus \Omega(A_i - C).$$

Assume now that A is of degree $\deg A < w$. Then there exists a nonzero linear combination f of $f_1, f_2, \ldots, f_w$ that vanishes on A (as a divisor, A is defined over the base field $\mathbb{F}$, with the possibility that some of the points in its support are defined over an extension of $\mathbb{F}$; in particular, f can be obtained as a nonzero solution to a system of $\deg A \leqslant w-1$ linear equations in w unknowns for a system of linear equations defined over $\mathbb{F}$). If f_i is the leading function in the linear combination then $f \in L(A_i - A) \setminus L(A_i - A - P)$ and $f\eta_i \in \Omega(-C - P + A) \setminus \Omega(-C + A)$. Thus $A - C \notin \Gamma_P$ and $A \notin \Gamma_P(C)$. □

Example 5.4. Let $\mathcal{C} = C_\Omega(D, K + 9P + 9Q)$ be the code of Example 2.5 and let $\mathcal{C}_1 = C_\Omega(D, K + 10P + 9Q)$ be a subcode of codimension one. We apply the theorem with $\Delta_P(C) = \Delta_P(9P + 9Q)$. An optimal strictly increasing sequence of divisors in $\Delta_P(C)$ is given by

$$A_1 = 0 \leqslant \cdots \leqslant A_{18} = 109P \leqslant A_{19} = 112P + 9Q \leqslant \cdots \leqslant A_{45} = 256P + 9Q.$$

The beginning of the sequence consists of all divisors $0 \leqslant A \leqslant 109P$ with $L(A) \neq L(A - P)$ and $L(A) = L(A - C)$. The remainder of the sequence consists of all divisors $112P + 9Q \leqslant A \leqslant 256P + 9Q$ with the same properties. It follows that $\gamma_P(C) \geqslant 45$, and thus, with Lemma 4.2, that words in $\mathcal{C} \setminus \mathcal{C}_1$ have weight at least 45.

For a divisor B, let

$$\begin{aligned} \Delta_P(B, C) &= \{B + iP\colon i \in \mathbb{Z}\} \cap \Delta_P(C) \\ &= \{B + iP \in \Gamma_P, B - C + iP \notin \Gamma_P\}. \end{aligned}$$

Lemma 5.5. *To the set* $\Delta_P(B, C)$ *corresponds a dual set*

$$\begin{aligned} \Delta_P(B - C, -C) &= \{B - C + iP\colon i \in \mathbb{Z}\} \cap \Delta_P(-C) \\ &= \{B - C + iP \in \Gamma_P, B + iP \notin \Gamma_P\}, \end{aligned}$$

such that $\#\Delta_P(B,C) - \#\Delta_P(B-C,-C) = \deg C$. *Furthermore,*

$$\#\Delta_P(B,C) = \begin{cases} \deg C, & \text{if } C \in \Gamma_P, \\ 0, & \text{if } -C \in \Gamma_P. \end{cases}$$

In particular,

$$\#\Delta_P(B,C) = \begin{cases} \deg C, & \text{if } \deg C \geqslant 2g, \\ 0, & \text{if } \deg C \leqslant -2g. \end{cases}$$

Proof. For i_0 large enough,

$$\begin{aligned} &\#\Delta_P(B,C) - \#\Delta_P(B-C,-C) \\ &\quad = \#\{i \leqslant i_0 \colon B + iP \in \Gamma_P,\ B - C + iP \notin \Gamma_P\} \\ &\qquad - \#\{i \leqslant i_0 \colon B + iP \notin \Gamma_P,\ B - C + iP \in \Gamma_P\} \\ &\quad = \sum_{i \leqslant i_0} \big(l(B+iP) - l(B+iP-P)\big) - \big(l(B-C+iP) - l(B-C+iP-P)\big) \\ &\quad = \dim L(B+i_0P) - \dim L(B-C+i_0P) = \deg C. \end{aligned}$$

For the remainder use Lemma 5.1. □

Corollary 5.6. *For any choice of divisor* B, *there is a pair of equivalent bounds*

$$\gamma_P(C) \geqslant \#\Delta_P(B,C), \qquad \gamma_P(-C) \geqslant \#\Delta_P(B-C,-C).$$

Proof. For the first inequality, the elements $A_1, A_2, \ldots, A_w \in \Delta_P(B,C)$, ordered from lowest to highest degree, meet the conditions of the theorem. Similar for the second inequality. Equivalence follows from $\gamma_P(C) - \gamma_P(-C) = \deg C$ and the previous lemma. □

Example 5.7. Let $\mathcal{C}/\mathcal{C}_1 = C_\Omega(D, K + 9P + 9Q)/C_\Omega(D, K + 10P + 9Q)$ as in Example 5.4. The corollary restricts the choice of a sequence of divisors in $\Delta_P(C) = \Delta_P(9P + 9Q)$ to sequences that increase by P at each step. Under the restriction, an optimal strictly increasing sequence of divisors in $\Delta_P(C)$ is given by

$$\Delta_P(0, 9P + 9Q) = \{A_1 = 0 \leqslant \cdots \leqslant A_{40} = 256P\}.$$

The sequence is of length 40 and the corollary therefore yields $d(\mathcal{C}/\mathcal{C}_1) \geqslant 40$.

Lemma 5.8. *If* $A \in \Gamma_P(E)$ *and* $E \in \Gamma_P(C)$ *then* $A \in \Gamma_P(C)$. *For* $E \in \Gamma_P(C)$,

$$\Delta_P(C) \subset \Delta_P(E).$$

Proof. The first claim is immediate from the definitions, in particular $A - E \in \Gamma_P$ and $E - C \in \Gamma_P$ implies $A - C \in \Gamma_P$. For $E \in \Gamma_P(C)$, the first claim shows that $A \notin \Gamma_P(E)$ whenever $A \notin \Gamma_P(C)$. □

6. Order bound and floor bound

We unify and improve two known lower bounds for the minimum distance of an algebraic geometric code. Let S be a given set of rational points, and let $C_L(D,G)$ and $C_\Omega(D,G)$ be algebraic geometric codes defined with a divisor $D = P_1 + \cdots + P_n$ disjoint from S. With Lemma 4.3,

$$d\big(C_L(D,G)\big) \geqslant \gamma^*(C;S), \quad \text{for } C = D - G,$$
$$d\big(C_\Omega(D,G)\big) \geqslant \gamma^*(C;S), \quad \text{for } C = G - K.$$

Proposition 6.1. *For rational points $Q_0,\dots,Q_{r-1} \in S$, define divisors $C_0 \leqslant C_1 \leqslant \cdots \leqslant C_r$ such that $C_0 = C$ and $C_{i+1} = C_i + Q_i$, for $i = 0,\dots,r-1$. Then*

$$\gamma^*(C;S) \geqslant \min\big\{\gamma_{Q_0}(C_0;S), \gamma_{Q_1}(C_1;S), \dots, \gamma_{Q_{r-1}}(C_{r-1};S), \gamma^*(C_r;S)\big\} \setminus \{0\}.$$

In general, $\gamma^*(C_r;S) \geqslant \deg C + r$.

Proof. Proposition 4.5 gives $\gamma^*(C_i;S) \geqslant \min\{\gamma_{Q_i}(C_i;S), \gamma^*(C_{i+1};S)\} \setminus \{0\}$. □

We give a formulation of the Beelen order bound for an algebraic geometric code $C_\Omega(D,G)$ in the notation of the current paper. The theorem is given in its general form (combining [3, Remark 5, Definition 6, Theorem 7]).

Theorem 6.2 *(Order bound). (See [3].) Let $C_\Omega(D,G)$ be an algebraic geometric code, and let $G = K + C$. For a sequence of rational points $Q_0,\dots,Q_{r-1}$ disjoint from D, let $C_0 = C$ and $C_{i+1} = C_i + Q_i$, for $i = 0,\dots,r-1$.*

$$\mathcal{C}_0 = C_\Omega(D, K + C) \supseteq \mathcal{C}_1 = C_\Omega(D, K + C_1) \supseteq \cdots \supseteq \mathcal{C}_r = C_\Omega(D, K + C_r).$$

If $\mathcal{C}_i \neq \mathcal{C}_{i+1}$ then a word in $\mathcal{C}_i \setminus \mathcal{C}_{i+1}$ has weight $w \geqslant \#\Delta_{Q_i}(0, C_i)$. For r large enough,

$$d\big(C_\Omega(D,G)\big) \geqslant \min\big\{\#\Delta_{Q_i}(0,C_i)\colon \mathcal{C}_i \neq \mathcal{C}_{i+1}\big\}.$$

More generally, for divisors $B_0,\dots,B_{r-1}$,

$$d\big(C_\Omega(D,G)\big) \geqslant \min\big\{\#\Delta_{Q_i}(B_i,C_i)\colon \mathcal{C}_i \neq \mathcal{C}_{i+1}\big\}.$$

Proof. The order bound for the minimum distance combines Proposition 6.1 with the estimates $\gamma_{Q_i}(C_i;S) \geqslant \gamma_{Q_i}(C_i) \geqslant \#\Delta_{Q_i}(B_i,C_i)$ in Corollary 5.6. □

The last part of the theorem allows a choice of divisors $B_0,\dots,B_r$. The original formulation has as extra condition that those divisors are disjoint from the divisor D but this condition is not necessary. We analyze the choice of the rational points $Q_0, Q_1, \dots, Q_{r-1}$. In [3], the choice of the points is unrestricted, and an example is given where the optimal lower bound is obtained with a choice of Q_i outside G. On the other hand, Proposition 4.1 shows that $\gamma_{Q_i}(C_i) \geqslant \deg C_i$. Thus, we may assume that the minimum $\min\{\gamma_{Q_i}(C_i)\} \setminus \{0\}$ is taken over an interval $i = 0, 1, \dots, r$ such that, for all i in the interval, either $\gamma_{Q_i}(C_i) = 0$ or $\gamma_{Q_i}(C_i) > \deg C_i$. With Proposition 4.1 this implies that either $-C_i \in \Gamma_{Q_i}$ or $C_i \notin \Gamma_{Q_i}$. In both cases, we can conclude, for $C_i \neq 0$, that $C_i \notin \Gamma_{Q_i}$, i.e. that $L(C_i) = L(C_i - Q_i)$. The same conclusion can be reached with Lemma 5.5 if the argument is repeated for $\Delta_{Q_i}(B_i,C_i)$ instead of $\gamma_{Q_i}(C_i)$. The following stronger result holds.

Proposition 6.3. *The maximum in the order bound is attained for a choice of rational points $Q_0, Q_1, \ldots, Q_{r-1}$ such that, for $i = 0, 1, \ldots, r-1$, either $C_i = 0$, or $Q_i, \ldots, Q_{r-1}$ are base points of the divisor C_i. In particular, if C_i is a nonzero effective divisor, we may restrict the choice for $Q_i, \ldots, Q_{r-1}$ to rational points in the support of C_i.*

Proof. For $Q \in \{Q_i, \ldots, Q_{r-1}\}$, let j be minimal in $\{i, \ldots, r-1\}$ such that $Q_j = Q$. If $C_j \neq 0$, we may assume as explained above, that $C_j \notin \Gamma_Q$. With $E = Q_i + \cdots + Q_{j-1} \in \Gamma_Q$ and $C_j = C_i + E$ it follows that $C_i \notin \Gamma_Q$. If $C_j = 0$ then either $i = j$, in which case $C_i = 0$, or $i < j$, in which case $\deg C_i < 0$ and $C_i \notin \Gamma_Q$. □

In [3, Example 8], the minimum distance lower bound for a code $C_\Omega(D, 5P)$ on the Klein curve is improved with a choice $Q_0 = P$, $Q_1 = Q \neq P$. For the example, $5P = K + 2P - Q$ and $6P = K + Q + R$, so that $C_0 = 2P - Q$ and $C_1 = Q + R$. Indeed, with the proposition, we can expect improvements only with $Q_1 = Q$ or with $Q_1 = R$.

To improve the order bound we apply the main theorem with a different format for the divisors $A_1, \ldots, A_w$. Let

$$\Delta_P(\leqslant B, C) = \{B + iP \in \Gamma_P\colon\ B - C + iP \notin \Gamma_P \wedge i \leqslant 0\},$$

$$\Delta_P(\geqslant B + P, C) = \{B + iP \in \Gamma_P\colon\ B - C + iP \notin \Gamma_P \wedge i \geqslant 1\},$$

be a partition of the set $\Delta_P(B, C)$ into divisors of small and large degree.

Lemma 6.4.

$$\#\Delta_P(\leqslant B, C) = \dim L(B) - \dim L(B - C) + \#\Delta_P(\leqslant B - C, -C).$$

Proof. Similar to the proof of Lemma 5.5, but use $i_0 = 0$. □

Theorem 6.5 *(ABZ bound for cosets). Let C be a divisor and let P be a rational point. For $G = K + C = A + B + Z$, $Z \geqslant 0$,*

$$\gamma_P(C; Z \cup P) \geqslant \#\Delta_P(\leqslant A, C) + \#\Delta_P(\leqslant B, C).$$

Proof. With Lemma 5.2, a divisor $A' \in \Delta_P(C)$ if and only if $K + C + P - A' \in \Delta_P(C)$. And $A' \leqslant A$ if and only if $K + C + P - A' \geqslant K + C + P - A = B + P + Z$. The elements $A_1, A_2, \ldots, A_w \in \Delta_P(\leqslant B, C) \cup \Delta_P(\geqslant B + P + Z, C)$, ordered from lowest to highest degree, meet the conditions of Theorem 5.3, with $w = \#\Delta_P(\leqslant A, C) + \#\Delta_P(\leqslant B, C)$. □

Example 6.6. As in Example 5.7, let $\mathcal{C} = C_\Omega(D, K + 9P + 9Q)$ and let $\mathcal{C}_1 = C_\Omega(D, K + 10P + 9Q)$. We apply the order bound with $B_0 = B_1 = \cdots = B_{35} = 0$, $Q_0 = Q_1 = \cdots = Q_{17} = P$, and $Q_{18} = Q_{19} = \cdots = Q_{35} = Q$. Example 5.7 gives the lower bound $d(\mathcal{C}/\mathcal{C}_1) \geqslant \#\Delta_P(0, 9P + 9Q) = 40$. Similarly, for $\mathcal{C}_{18} = C_\Omega(D, K + 27P + 9Q)$,

$$d(\mathcal{C}_1/\mathcal{C}_{18}) \geqslant \min\bigl\{\#\Delta_P(0, 10P + 9Q), \ldots, \#\Delta_P(0, 26P + 9Q)\bigr\} = 50.$$

And, for $C_{36} = C_\Omega(D, K + 27P + 27Q)$,

$$d(\mathcal{C}_{18}/\mathcal{C}_{36}) \geqslant \min\bigl\{\#\Delta_Q(0, 27P + 9Q), \ldots, \#\Delta_Q(0, 27P + 26Q)\bigr\} = 54.$$

The Goppa bound gives $d(C_{36}) \geqslant 54$, and it follows that $d(\mathcal{C}_{18}) \geqslant 54$, $d(\mathcal{C}_1) \geqslant 50$, and $d(\mathcal{C}) \geqslant 40$. The last three values are best possible for the order bound. Example 5.4 shows that $d(\mathcal{C}/\mathcal{C}_1) \geqslant 45$ and thus $d(\mathcal{C}) \geqslant 45$. The sequence of divisors that was used to obtain the lower bound,

$$A_1 = 0 \leqslant \cdots \leqslant A_{18} = 109P \leqslant A_{19} = 112P + 9Q \leqslant \cdots \leqslant A_{45} = 256P + 9Q,$$

matches the format of the ABZ bound for cosets, with $K + C = A + B + Z$ for $K = 246P$, $C = 9P + 9Q$, $A = 146P$, $B = 109P$, $Z = 9Q$, and $\#\Delta_P(\leqslant A, C) + \#\Delta_P(\leqslant B, C) = 27 + 18 = 45$.

The lower bound $\#\Delta_P(B, C)$ that is used for the order bound takes into account only the number of divisors in a delta set $\Delta_P(B, C)$. The improved bounds in Theorem 6.5 are possible by considering also the degree distribution of divisors in the delta set. For $Z = 0$, the bounds in the theorem include those used in the order bound (Theorem 6.2). The floor bound (Theorem 2.3) sometimes exceeds the order bound. The ABZ bound for codes (Theorem 2.4) gives an improvement and generalization of the floor bound. We show that the bounds in the theorem not only include those obtained with the order bound but also those obtained with the ABZ bound for codes. In each case, the coset decoding procedure in Appendix A decodes efficiently up to half the bound.

Theorem 6.7 *(ABZ bound for codes). Let $G = K + C = A + B + Z$, for $Z \geqslant 0$. For D with $D \cap Z = \emptyset$, a nonzero word in $C_\Omega(D, G)$ has weight $w \geqslant l(A) - l(A - C) + l(B) - l(B - C)$.*

Proof. Let P be a rational point on the curve not in the support of D, if necessary it can be chosen over an extension field. We use Proposition 6.1 with $S = Z \cup P$ and $Q_0 = Q_1 = \cdots = Q_{r-1} = P$.

$$\gamma^*(C; S) \geqslant \min\{\gamma_P(C; S), \gamma_P(C + P; S), \ldots, \gamma_P\big(C + (r-1)P; S\big), \gamma^*(C + rP; S)\} \setminus \{0\}.$$

Now use Theorem 6.5 with $K + C + iP = A + B + (Z + iP)$,

$$\gamma_P(C + iP; S) \geqslant \#\Delta_P(\leqslant A, C + iP) + \#\Delta_P(\leqslant B, C + iP).$$

With Lemma 6.4,

$$\begin{aligned}\gamma_P(C + iP; S) &\geqslant l(A) - l(A - C - iP) + l(B) - l(B - C - iP)\\ &\geqslant l(A) - l(A - C) + l(B) - l(B - C).\end{aligned}$$

Hence, by taking r large enough, $\gamma^*(C; S) \geqslant l(A) - l(A - C) + l(B) - l(B - C)$. □

Neither the ABZ bound for codes, nor the ABZ bound for cosets gives an improvement in general. For $Z = 0$, both bounds return previously known bounds, namely the Goppa bound and the order bound, respectively. For carefully chosen nontrivial Z, there are possible improvements. If we apply Lemma 6.4 with both A and B,

$$\begin{aligned}\#\Delta_P(\leqslant A, C) &= \dim L(A) - \dim L(A - C) + \#\Delta_P(\leqslant A - C, -C),\\ \#\Delta_P(\leqslant B, C) &= \dim L(B) - \dim L(B - C) + \#\Delta_P(\leqslant B - C, -C),\end{aligned}$$

and add the two equations, then we see that the improvement of the ABZ coset bound applied to $G = K + C = A + B + Z$ over the floor bound applied to $G = K + C = A + B + Z$ is given by the ABZ coset bound applied to the dual decomposition $G' = K - C = (A - C) + (B - C) + Z$. For $Z = 0$, we recover that the improvement of the order bound applied to $G = K + C$ over the Goppa bound $\deg C$ is given by the order bound applied to $G' = K - C$ (Lemma 5.5 and Corollary 5.6).

Example 6.8. As in Example 6.6, let $\mathcal{C} = C_\Omega(D, K + 9P + 9Q)$ and let $\mathcal{C}_1 = C_\Omega(D, K + 10P + 9Q)$. The ABZ bound for codes in Example 2.5 gives $d(\mathcal{C}) \geqslant 28$, for $A = 4H = 164P$, $B = 2H = 82P$, $Z = 9P + 9Q$. For this choice of A, B and Z, the ABZ bound for cosets gives $d(\mathcal{C}/\mathcal{C}_1) \geqslant 31 + 12 = 43$.

$$\#\Delta_P(\leqslant A, C) = 31, \qquad \dim L(A) - \dim L(A - C) = 18, \qquad \#\Delta_P(\leqslant A - C, -C) = 13,$$
$$\#\Delta_P(\leqslant B, C) = 12, \qquad \dim L(B) - \dim L(B - C) = 10, \qquad \#\Delta_P(\leqslant B - C, -C) = 2.$$

The ABZ bound for cosets in Example 6.6 gives $d(\mathcal{C}/\mathcal{C}_1) \geqslant 45$, for $A = 146P$, $B = 109P$, $Z = 9Q$. For this choice of A, B and Z, the ABZ bound for codes gives $d(\mathcal{C}) \geqslant 14 + 11 = 25$.

$$\#\Delta_P(\leqslant A, C) = 27, \qquad \dim L(A) - \dim L(A - C) = 14, \qquad \#\Delta_P(\leqslant A - C, -C) = 13,$$
$$\#\Delta_P(\leqslant B, C) = 18, \qquad \dim L(B) - \dim L(B - C) = 11, \qquad \#\Delta_P(\leqslant B - C, -C) = 7.$$

In general, the ABZ bound for cosets $d(\mathcal{C}/\mathcal{C}_1)$ is at least the ABZ bound for codes $d(\mathcal{C})$, for the same choice of A, B and Z. But the optimal choices for A, B and Z need not be the same for the two bounds.

We consider the special case of the order bound with $B_0 = \cdots = B_{r-1} = 0$ and $Q_0 = \cdots = Q_{r-1} = P$. For codes of the form $C_L(D, \rho P)^\perp = C_\Omega(D, \rho P)$ or of the form $C_L(D, K + P + \rho P)^\perp = C_\Omega(D, K + P + \rho P)$ the resulting bound can be formulated entirely in terms of the numerical semigroup H of Weierstrass P-nongaps. For the first code use $C = \rho P - K$, and for the second $C = \rho P + P$. For the delta sets we obtain

$$\begin{aligned} pP \in \Delta_P(\rho P - K) \quad &\Leftrightarrow \quad pP \in \Gamma_P \wedge K + pP - \rho P \notin \Gamma_P \\ &\Leftrightarrow \quad p \in H \wedge \rho - p + 1 \in H, \\ pP \in \Delta_P(\rho P + P) \quad &\Leftrightarrow \quad pP \in \Gamma_P \wedge pP - \rho P - P \notin \Gamma_P \\ &\Leftrightarrow \quad p \in H \wedge p - \rho - 1 \notin H. \end{aligned}$$

The first of the two bounds in the following theorem is the Feng–Rao bound [11,12]. The second bound is different when the canonical divisor $K \not\sim (2g - 2)P$.

Theorem 6.9 *(Feng–Rao bound). Let H be the semigroup of Weierstrass P-nongaps.*

$$d\big(C_L(D, \rho P)^\perp\big) \geqslant \min\big\{\#A\big[\rho'\big]\colon \rho' > \rho\big\} \setminus \{0\},$$

where $A[\rho] = \{p \in H \mid \rho - p \in H\}$.

$$d\big(C_L(D, K + \rho P + P)^\perp\big) \geqslant \min\big\{\#B\big[\rho'\big]\colon \rho' > \rho\big\} \setminus \{0\},$$

where $B[\rho] = \{p \in H \mid p - \rho \notin H\}$.

Proof. Apply Proposition 6.1 with the given delta sets. □

7. Concluding remark

Both problems of finding the lower bound for the adversary threshold of an algebraic geometric linear secret sharing scheme and the lower bound for the minimum distance of an algebraic geometric code can be approached as a geometric approximation problem: Given a divisor on an algebraic curve, represent the divisor as a difference of two effective divisors such that the effective divisors are each disjoint from a given set S and find lower bounds for the degrees of the effective divisors in such a representation. In other words, for a given curve X and divisor class C, find the lower bounds on the degree of a divisor A such that A and $A - C$ belong to specified semigroups of divisors. For suitable choices of the semigroups we obtain (1) lower bounds for the size of a party A that can recover the secret in an algebraic geometric linear secret sharing scheme with adversary threshold C, and (2) lower bounds for the support A of a codeword in a geometric Goppa code with designed minimum support C.

Appendix A. Coset decoding

For a given vector $y \in \mathbb{F}^n$, and for an extension of linear codes $\mathcal{C}' \subset \mathcal{C} \subset \mathbb{F}^n$, coset decoding determines the cosets of $\mathcal{C}'$ in $\mathcal{C}$ that are nearest to the vector y. If y is at distance $d(y, \mathcal{C}) \leqslant t$ from $\mathcal{C}$ and the minimum distance $d(\mathcal{C}/\mathcal{C}')$ between distinct cosets is at least $w > 2t$ then there exists a unique nearest coset $c + \mathcal{C}'$ with $d(y, c + \mathcal{C}') \leqslant t$. We describe a coset decoding procedure that returns the unique coset when the estimate $d(\mathcal{C}/\mathcal{C}') \geqslant w$ is obtained with Theorem 1.2. The procedure follows the majority coset decoding procedure in [13,14].

Shift bound or coset bound (Theorem 1.2): Let $\mathcal{C}/\mathcal{C}_1$ be an extension of $\mathbb{F}$-linear codes with corresponding extension of dual codes $\mathcal{D}_1/\mathcal{D}$ such that $\dim \mathcal{C}/\mathcal{C}_1 = \dim \mathcal{D}_1/\mathcal{D} = 1$. If there exist vectors $a_1, \ldots, a_w$ and $b_1, \ldots, b_w$ such that

$$\begin{cases} a_i * b_j \in \mathcal{D} & \text{for } i + j \leqslant w, \\ a_i * b_j \in \mathcal{D}_1 \setminus \mathcal{D} & \text{for } i + j = w + 1, \end{cases}$$

then $d(\mathcal{C}/\mathcal{C}_1) \geqslant w$.

For a given $x \in \mathcal{D}_1 \setminus \mathcal{D}$, we may assume, after rescaling if necessary, that $a_i * b_{w+1-i} \in x + \mathcal{D}$, for $i = 1, \ldots, w$. Define the following cosets of a_i and b_{w+1-i}, for $i = 1, \ldots, w$,

$$A_i = a_i + \langle a_1, \ldots, a_{i-1} \rangle,$$

$$B_{w+1-i} = b_{w+1-i} + \langle b_1, \ldots, b_{w-i} \rangle.$$

For $c \in \mathcal{C}$, the coset $c + \mathcal{C}_1$ is uniquely determined by $x \cdot c$. For a given $y \in \mathbb{F}^n$ such that $d(y, \mathcal{C}) \leqslant t$, the decoding procedure will look for a pair $a' \in A_i$, $b' \in B_{w+1-i}$ such that, for all $c \in \mathcal{C}$ with $d(y, c) \leqslant t$, $(a' * b') \cdot y = x \cdot c$. The vector $a' * b'$ is defined as the Hadamard or coordinate-wise product of the vectors a' and b'. We use $(a' * b') \cdot y = (a' * y) \cdot b'$.

Theorem A.1 *(Decoding up to half the coset bound). Let $2t < w \leqslant d(\mathcal{C}/\mathcal{C}_1)$, for $\mathcal{C}/\mathcal{C}_1$ and w as in Theorem 1.2. For $y \in \mathbb{F}^n$ such that $d(y, \mathcal{C}) \leqslant t$, let*

$$I = \left\{ 1 \leqslant i \leqslant w \colon \left(\exists a'_i \in A_i\right)\left(a'_i * b_j\right) \perp y,\ 1 \leqslant j \leqslant w - i \right\},$$

$$I^* = \left\{ 1 \leqslant j \leqslant w \colon \left(\exists b'_j \in B_{w+1-j}\right)\left(a_i * b'_j\right) \perp y,\ 1 \leqslant i \leqslant j - 1 \right\}.$$

For every $c \in \mathcal{C}$ with $d(y, c) \leqslant t$, $x \cdot c = (a'_i * b'_i) \cdot y$, for a majority of $i \in I \cap I^*$.

Proof. For $c \in \mathcal{C}$, let $a_i' \in A_i$ be such that $a_i' * y = a_i' * c$. The vector a_i', if it exists, satisfies $(a_i' * b_j) \cdot y = 0$, for $j = \{1, \ldots, w-i\}$. Moreover, for any $b' \in B_{w+1-i}$, $(a_i' * b') \cdot y = (a_i' * b') \cdot c = (a_i * b_{w+1-i}) \cdot c = x \cdot c$. Let

$$\Gamma = \{1 \leqslant i \leqslant w\colon (\exists a_i' \in A_i) a_i' * y = a_i' * c\}, \qquad \Delta = \{1 \leqslant i \leqslant w\} \setminus \Gamma,$$
$$\Gamma^* = \{1 \leqslant j \leqslant w\colon (\exists b_j' \in B_{w+1-j}) b_j' * y = b_j' * c\}, \qquad \Delta^* = \{1 \leqslant j \leqslant w\} \setminus \Gamma^*.$$

We know a priori only the sets I and I^*. Clearly, $\Gamma \subset I$ and $\Gamma^* \subset I^*$. Moreover, for $c \in \mathcal{C}$ with $d(y, c) \leqslant t$, $|\Delta|, |\Delta^*| \leqslant t$. For $i \in I \cap I^*$, $(a_i' * b_i') \cdot y = x \cdot c$ if either $i \in \Gamma$ or $i \in \Gamma^*$. Regardless of the actual sets I and I^*, this is certainly the case if $i \in \Gamma \cap \Gamma^*$ and it fails only when $i \in \Delta \cap \Delta^*$. Now

$$\left|\Gamma \cap \Gamma^*\right| - \left|\Delta \cap \Delta^*\right| = w - \left|\Gamma \cap \Delta^*\right| - \left|\Gamma^* \cap \Delta\right| \geqslant w - 2t > 0.$$

Thus, the majority of $i \in I \cap I^*$ will give a value $(a_i' * b_i') \cdot y = x \cdot c$. □

If $\dim \mathcal{C}/\mathcal{C}' > 1$ then the procedure can be applied iteratively to a sequence of extensions $\mathcal{C}' = \mathcal{C}_r \subset \mathcal{C}_{r-1} \subset \cdots \mathcal{C}_1 \subset \mathcal{C}_0 = \mathcal{C}$ such that $\dim \mathcal{C}_i/\mathcal{C}_{i-1} = 1$, for $i = 1, \ldots, r$. For given $y_0 \in \mathbb{F}^n$ with $d(y_0, \mathcal{C}_0) \leqslant t$, the procedure returns the unique coset $c_0 + \mathcal{C}_1$ such that $d(y_0, c_0 + \mathcal{C}_1) \leqslant t$. At the next iteration, for $y_1 = y_0 - c_0 \in \mathbb{F}^n$ with $d(y_1, \mathcal{C}_1) \leqslant t$, the procedure returns the unique coset $c_1 + \mathcal{C}_2$ such that $d(y_1, c_1 + \mathcal{C}_2) \leqslant t$, and so on.

Let $\mathcal{A} = \{A_1 \leqslant A_2 \leqslant \cdots \leqslant A_w\} \subset \Delta_P(C)$ be a sequence of divisors with $A_{i+1} \geqslant A_i + P$, for $i = 1, \ldots, w-1$. Theorem 5.3 (Main theorem) together with Lemma 4.2 shows that $d(C_\Omega(D, G-P)/C_\Omega(D, G)) \geqslant w$, for G such that $C = G - K - P$, and for $D \cap (A_w - A_1) = \emptyset$. We show how the coset decoding procedure applies to the given extension. For a divisor $A_i \in \Delta_P(C)$, also $K + C + P - A_i = G - A_i \in \Delta_P(C)$. Thus, there exist functions $f_i \in L(A_i) \setminus L(A_i - P)$ and $g_i \in L(G - A_i) \setminus L(G - A_i - P)$. Let $(a_i * b_{w+1-j}) = ((f_i g_j)(P_n), \ldots, (f_i g_j)(P_n))$, for $i \leqslant j$. Then

$$\begin{cases} a_i * b_j \in C_L(D, G) & \text{for } i + j \leqslant w, \\ a_i * b_j \in C_L(D, G) \setminus C_L(D, G - P) & \text{for } i + j = w + 1. \end{cases}$$

Moreover, we have the following interpretation for the sets $\Gamma, \Gamma^*, \Delta, \Delta^*$.

$$i \in \Gamma \quad \Leftrightarrow \quad A_i \in \Gamma_P(Q), \qquad i \in \Delta \quad \Leftrightarrow \quad A_i \in \Delta_P(Q),$$
$$i \in \Gamma^* \quad \Leftrightarrow \quad A_i \in \Delta_P(C - Q), \qquad i \in \Delta^* \quad \Leftrightarrow \quad A_i \in \Gamma_P(C - Q).$$

Here the divisor Q, for $0 \leqslant Q \leqslant D$, denotes the support of the error vector $y - c$. The order bound (Theorem 6.2) and the floor bound (Theorem 2.3) as well as their generalizations the ABZ bound for cosets (Theorem 6.5) and the ABZ bound for codes (Theorem 6.7) are all obtained in this paper as special cases of the main theorem. Thus, in each case coset decoding can be performed with Theorem A.1.

Appendix B. Notation

(Section 1) $\{1, 2, \ldots, n\} = \Gamma(\mathcal{D}_1/\mathcal{D}) \cup \Delta(\mathcal{D}_1/\mathcal{D})$: For an extension of $\mathbb{F}$-linear codes $\mathcal{D}_1 \supset \mathcal{D}$ of length n, the coordinate set $\{1, 2, \ldots, n\}$ is partitioned into qualified subsets $\Gamma(\mathcal{D}_1/\mathcal{D})$ and unqualified subsets $\Delta(\mathcal{D}_1/\mathcal{D})$. With Theorem 1.6, the partition is such that a subset $A \subset \{1, 2, \ldots, n\}$ belongs to $\Gamma(\mathcal{D}_1/\mathcal{D})$ if every word in the difference $\mathcal{D}_1 \setminus \mathcal{D}$ has at least one nonzero coordinate in A and it belongs to $\Delta(\mathcal{D}_1/\mathcal{D})$ otherwise.

(Section 4) $\Gamma_P = \Gamma_P(C) \cup \Delta_P(C)$: For a rational point P, Γ_P is the semigroup of divisor classes A with no base point at P, that is to say with $L(A) \neq L(A - P)$. For a divisor C, the semigroup Γ_P is partitioned into $\Gamma_P(C)$ and $\Delta_P(C)$, with

$$\Gamma_P(C) = \{A\colon\ L(A) \neq L(A-P) \wedge L(A-C) \neq L(A-C-P)\},$$
$$\Delta_P(C) = \{A\colon\ L(A) \neq L(A-P) \wedge L(A-C) = L(A-C-P)\}.$$

For a finite set of rational points S, and for a rational point $P \in S$,

$$\Gamma_S = \bigcap_{Q \in S} \Gamma_Q,$$
$$\Gamma_P(C;S) = \Gamma_P(C) \cap \Gamma_S = \{A \in \Gamma_S\colon\ A - C \in \Gamma_P\},$$
$$\Gamma(C;S) = \{A \in \Gamma_S\colon\ L(A-C) \neq 0\},$$
$$\Gamma^*(C;S) = \{A \in \Gamma_S\colon\ L(A-C) \neq L(-C)\}.$$

References

[1] Masaaki Homma, Seon Jeong Kim, The complete determination of the minimum distance of two-point codes on a Hermitian curve, Des. Codes Cryptogr. 40 (1) (2006) 5–24.
[2] Hao Chen, Ronald Cramer, Algebraic geometric secret sharing schemes and secure multi-party computations over small fields, in: Advances in Cryptology—CRYPTO 2006, in: Lecture Notes in Comput. Sci., vol. 4117, Springer, Berlin, 2006, pp. 521–536.
[3] Peter Beelen, The order bound for general algebraic geometric codes, Finite Fields Appl. 13 (3) (2007) 665–680.
[4] Benjamin Lundell, Jason McCullough, A generalized floor bound for the minimum distance of geometric Goppa codes, J. Pure Appl. Algebra 207 (1) (2006) 155–164.
[5] C. Güneri, H. Stichtenoth, I. Taskin, Further improvements on the designed minimum distance of algebraic geometry codes, J. Pure Appl. Algebra 213 (1) (2009) 87–97.
[6] Seungkook Park, Applications of algebraic curves to cryptography, Dissertation, University of Illinois, Urbana, 2007.
[7] Ronald Cramer, Ivan Damgård, Ueli Maurer, General secure multi-party computation from any linear secret-sharing scheme, in: Advances in Cryptology—EUROCRYPT 2000, Bruges, in: Lecture Notes in Comput. Sci., vol. 1807, Springer, Berlin, 2000, pp. 316–334.
[8] Ronald Cramer, Vanesa Daza, Ignacio Gracia, Jorge Jiménez Urroz, Gregor Leander, Jaume Martí-Farré, Carles Padró, On codes, matroids and secure multi-party computation from linear secret sharing schemes, in: Advances in Cryptology—CRYPTO 2005, in: Lecture Notes in Comput. Sci., vol. 3621, Springer, Berlin, 2005, pp. 327–343.
[9] Iwan M. Duursma, Seungkook Park, Coset bounds for algebraic geometric codes, arXiv:0810.2789, 2008.
[10] Jacobus H. van Lint, Richard M. Wilson, On the minimum distance of cyclic codes, IEEE Trans. Inform. Theory 32 (1) (1986) 23–40.
[11] Gui Liang Feng, T.R.N. Rao, Decoding algebraic–geometric codes up to the designed minimum distance, IEEE Trans. Inform. Theory 39 (1) (1993) 37–45.
[12] Antonio Campillo, José Ignacio Farrán, Carlos Munuera, On the parameters of algebraic–geometry codes related to Arf semigroups, IEEE Trans. Inform. Theory 46 (7) (2000) 2634–2638.
[13] Iwan M. Duursma, Decoding codes from curves and cyclic codes, Dissertation, Technische Universiteit Eindhoven, Eindhoven, 1993.
[14] Iwan M. Duursma, Majority coset decoding, IEEE Trans. Inform. Theory 39 (3) (1993) 1067–1070.

Further reading

[15] Christoph Kirfel, Ruud Pellikaan, The minimum distance of codes in an array coming from telescopic semigroups, IEEE Trans. Inform. Theory 41 (6, part 1) (1995) 1720–1732, special issue on algebraic geometry codes.
[16] Michael E. O'Sullivan, New codes for the Berlekamp–Massey–Sakata algorithm, Finite Fields Appl. 7 (2) (2001) 293–317.
[17] Cícero Carvalho, Fernando Torres, On Goppa codes and Weierstrass gaps at several points, Des. Codes Cryptogr. 35 (2) (2005) 211–225.
[18] Hiren Maharaj, Gretchen L. Matthews, On the floor and the ceiling of a divisor, Finite Fields Appl. 12 (1) (2006) 38–55.
[19] Iwan M. Duursma, Algebraic geometry codes: General theory, in: C. Munuera, E. Martinez-Moro, D. Ruano (Eds.), Advances in Algebraic Geometry Codes, in: Ser. Coding Theory Cryptogr., World Scientific, 2008.
[20] W. Cary Huffman, Vera Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge, 2003.
[21] Oliver Pretzel, Codes and Algebraic Curves, Oxford Lecture Ser. Math. Appl., vol. 8, Clarendon Press, Oxford University Press, New York, 1998.
[22] Serguei A. Stepanov, Codes on Algebraic Curves, Kluwer Academic/Plenum Publishers, New York, 1999.
[23] Henning Stichtenoth, Algebraic Function Fields and Codes, second ed., Grad. Texts in Math., vol. 254, Springer-Verlag, Berlin, 2009.

[24] Michael Tsfasman, Serge Vlăduţ, Dmitry Nogin, Algebraic Geometric Codes: Basic Notions, Math. Surveys Monogr., vol. 139, Amer. Math. Soc., Providence, RI, 2007.
[25] J.H. van Lint, Introduction to Coding Theory, third ed., Grad. Texts in Math., vol. 86, Springer-Verlag, Berlin, 1999.